requirements to participate in the voluntary DIB CS/IA information sharing program as set forth in this part (see § 236.7).

(i) *Government* means the United States Government.

(j) *Government Furnished Information (GFI)* means information provided by the Government under the voluntary DIB CS/IA program, including but not limited to cyber threat information and information assurance practices.

(k) *Information* means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(l) *Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(m) *Threat* means any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

(n) *U.S. based* means provisioned, maintained, or operated within the physical boundaries of the United States.

(o) *U.S. citizen* means a person born in the United States or naturalized.

§ 236.3 Policy.

It is DoD policy to:

(a) Establish a comprehensive approach for enhancing and supplementing DIB information assurance capabilities to safeguard covered defense information on covered DIB systems.

(b) Increase the Government and DIB situational awareness of the extent and severity of cyber threats to DoD information.

§ 236.4 Procedures.

(a) The Government and each DIB participant will execute a voluntary standardized agreement, referred to as a Framework Agreement (FA), to share, in a timely and secure manner, on a recurring basis, and to the greatest extent possible, cyber security information relating to information assurance for covered defense information on covered DIB systems.

(b) Each such FA between the Government and a DIB participant must comply with and implement the requirements of this part, and will include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in this part with individual DIB participants.

(c) DoD's DIB CS/IA Program Office is the overall point of contact for the program. The DoD Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment (DC3/DCISE) is the operational focal point for cyber threat information sharing and incident reporting under the DIB CS/IA program.

(d) The Government will maintain a Web site or other Internet-based capability to provide potential DIB participants with information about eligibility and participation in the program, to enable the online application or registration for participation, and to support the execution of necessary agreements with the Government. *http://dibnet.dod.mil/*.

(e) Prior to receiving GFI from the Government, each DIB participant shall provide the requisite points of contact information, to include security clearance and citizenship information, for the designated personnel within their company (e.g., typically 3–10 company designated points of contact) in order to facilitate the DoD–DIB interaction in the DIB CS/IA program. The Government will confirm the accuracy of the information provided as a condition of that point of contact being authorized to act on behalf of the DIB participant for this program.

(f) GFI will be issued via both unclassified and classified means. DIB participant handling and safeguarding of classified information shall be in compliance with the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22–M). The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB participants of any